UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

A.D., N.D., I.D., and N.S.D., on behalf of themselves and all others similarly situated, by their parent and guardian, NICOLE DEMONTE, Plaintiffs, v. ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs A.D., N.D., I.D., and N.S.D., by their parent and guardian Nicole Demonte (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, bring this action against Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's" or "Defendant"). The following allegations are based on Plaintiffs' knowledge, investigations by counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. This class action arises out of a recent cyberattack and data breach (the "Data Breach") resulting from Lurie Children's failure to implement reasonable and industry-standard data security practices to protect its patients' personal identifying information, including personal health information ("PII/PHI").

2. Lurie Children's is a pediatric hospital located in Chicago, IL, and the largest pediatric hospital in the region. Every year, more than 239,000 children receive medical treatment at Lurie Children's. Lurie Children's advertises expertise in neurology and neurosurgery, neonatology, urology, gastroenterology, and other specialties. In providing

medical care to children and families from across the country, Lurie Children's collects, uses, and derives a benefit from its patients' extremely sensitive PII/PHI—and it assumes a significant duty to protect that information.

3. But Lurie Children's did not protect its patients' PII/PHI.

4. In January of this year, in a shocking cyberattack, thieves accessed, and reportedly exfiltrated, approximately 800,000 Lurie Children's patients' personal and medical information. The Data Breach resulted in the exposure and theft of, at a minimum, patients' names, addresses, dates of birth, dates of medical treatments, driver's licenses numbers, email addresses, health claims information, health plan information, health plan beneficiary numbers, medical conditions or diagnoses, medical record numbers, medical treatments, prescription information, Social Security numbers, and telephone numbers.

5. A criminal ransomware group, Rhysida, claimed that it had stolen and sold the data on the Dark Web for 60 bitcoins, or approximately $3.4 million.[1]

6. Even when Lurie Children's notified Plaintiffs and the Class Members of the Data Breach, it failed to adequately describe the Data Breach and its effects, as well as the measures it took to prevent future data breaches.

7. In its notice to patients, Lurie Children's admitted that "cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024."[2] But Lurie Children's did not explain how it could have allowed PII/PHI including medical information and social security numbers to be so easily accessed. And while it promised it was "working closely with security

[1] Giles Bruce, *Hackers say they sold Lurie Children's Hospital data for $3.4M*, Becher's Health IT (Mar. 8, 2024), https://www.beckershospitalreview.com/cybersecurity/hackers-say-they-sold-lurie-childrens-hospital-data-for-3-4m.html.
[2] Lurie Children's Notifies Individuals of Data Breach, https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/ (last accessed July 2, 2024).

experts to continue our ongoing efforts to further enhance the security of our systems," those vague statements do not confirm that Plaintiffs' or the Class Members' PII/PHI will be safe in the future.

8. Lurie Children's failed to protect Plaintiffs' and the Class Members' PII/PHI, which hackers targeted because of its value in exploiting and stealing Plaintiffs' and the Class Members' identities. Plaintiffs and the Class Members now face a risk of boundless financial crimes; the hackers now have the means to open new financial accounts in their names', take out loans using their identities, use their information to obtain medical services or government benefits, file fraudulent tax returns, obtain false drivers' licenses, and give false information to the police during an arrest—among other things. Plaintiffs and the Class Members must now suffer additional financial costs for purchasing protective measures including credit monitoring, credit freezes, credit reports, and other means of detecting and mitigating identity theft.

9. Plaintiffs and the Class Members have suffered, and will continue to suffer, from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII/PHI, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

10. Through this action, Plaintiffs seek to hold Lurie Children's accountable and remedy these injuries.

PARTIES

11. Plaintiff A.D., a minor, is a natural person residing in Chicago, Illinois. Plaintiff A.D. received a notice of the data breach from Lurie Children's.

12. Plaintiff N.D., a minor, is a natural person residing in Chicago, Illinois. Plaintiff N.D. received a notice of the data breach from Lurie Children's.

13. Plaintiff I.D., a minor, is a natural person residing in Chicago, Illinois. Plaintiff I.D. received a notice of the data breach from Lurie Children's.

14. Plaintiff N.S.D., a minor, is a natural person residing in Chicago, Illinois. Plaintiff N.S.D. received a notice of the data breach from Lurie Children's.

15. Lurie Children's is an Illinois not-for-profit corporation with a principal address at 225 East Chicago Avenue, Chicago, IL 60611.

JURISDICTION AND VENUE

16. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because members of the class are citizens of states different than that of Defendant.

17. This Court has personal jurisdiction over Lurie Children's because Lurie Children's maintains its principal place of business in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims in this case emanated from activities within this District, and because Lurie Children's maintains its principal place of business in this District.

FACTUAL ALLEGATIONS

A. Lurie Children's collected and kept consumers' PII/PHI.

19. Lurie Children's is a healthcare provider that specializes in radiology and radiology subspecialties. Lurie Children's advertises that it is the "#1" pediatric hospital in Illinois and boasts that it is staffed "by the very best pediatric specialists who understand kids

and will do whatever it takes to provide them with a healthier future."

20. In its business of providing medical services, Lurie Children's collects and stores' patients' personal information and medical information, including, at a minimum, names, addresses, Social Security numbers, health insurance information, and medical information. These records were and are stored on Lurie Children's networks.

B. Lurie Children's promised to protect patients' PII/PHI.

21. Because of the highly sensitive and personal nature of the information that Lurie Children's acquires and stores, Lurie Children's knew or reasonably should have known that it stored protected PII/PHI and must comply with industry standards related to data security, as well as all state and federal laws protecting consumers' PII/PHI.

22. In particular, as a pediatric hospital, Lurie Children's knew or should have known that protecting its minor patients' PII/PHI was of the utmost importance.

23. Lurie Children's promises its patients that it will protect PII/PHI from theft and misuse and represented to Plaintiffs and the Class Members that it would maintain reasonable security over Plaintiffs' and the Class Members' PII/PHI.

24. Lurie Children's website, for example, advertises a Notice of Privacy Practices ("Privacy Practices") that "describes how medical information about you pay be used and disclosed and how you can access this information."[3] The Privacy Practices describes Lurie Children's requirements under HIPAA[4] and acknowledges that Lurie Children's obtains patients'

[3] Notice of Privacy Practices, https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last accessed July 2, 2024).

[4] "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996, which, among other things, sets forth guidelines by which personal information maintained by entities operating in the healthcare and health insurance industries should be protected from fraud and theft.

PII/PHI. Lurie Children's promises to protect patient data, including the following express commitments[5]:

a. "We are required by law to . . . assure that patient information that identifies you is kept confidential in accordance with law."

b. "[W]e must obtain your written authorization to use or disclose your patient information" (other than for specific, enumerated uses).

25. Lurie Children's also maintains a Website Privacy Policy ("Website Policy")[6], which also promises to protect users' data:

a. "We are committed to protecting the privacy of children."

b. "Lurie Children's is committed to maintaining reasonable physical, technical, and administrative measures to protect your personal information."

c. "We will retain your personal data for as long as necessary to accomplish the purpose for which it was collected unless a longer period is required by law or needed to resolve a dispute or protect our legal rights."

26. Lurie Children's also promises that it will only share patients' PII/PHI in specific scenarios that are identified in the Privacy Practices and Website Policy, which are largely limited to uses related to the hospital's operations and patient care.

27. Other than these limited, enumerated scenarios, Lurie Children's promises that it will not release patients' PII/PHI to third parties.

28. At no time did Lurie Children's inform any Class Member that Lurie Children's did not use reasonable measures to protect PII/PHI from disclosure to third parties; did not use physical, technical, or administrative measures to protect personal information; did not keep patient information confidential; disclosed patient information without patient consent; and did not comply with state and federal laws pertaining to the confidentiality of personal and health-

[5] Notice of Privacy Practices, https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last accessed July 2, 2024).
[6] Website Privacy Policy (Aug. 28, 2023), https://www.luriechildrens.org/en/privacy-legal-information/website-privacy-policy/ (last accessed July 2, 2024).

related information.

C. Lurie Children's has a duty to protect patients' PII/PHI.

29. Apart from its own explicit promises, Lurie Children's has a separate duty to protect Plaintiffs' and the Class Members' PII/PHI. By obtaining, collecting, receiving, and storing Plaintiffs' and the Class Members' PII/PHI, Lurie Children's assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting that PII/PHI from unauthorized disclosure.

30. This was particularly so given that Lurie Children's patients are children.

31. Lurie Children's has obligations created by the FTC Act, HIPAA, and industry standards to keep its patients' PII/PHI confidential, to use it only for authorized business and healthcare purposes, and to protect it from unauthorized access and disclosure.

32. Cyberattacks have become so prevalent that the FBI and U.S. Secret Service have issued warnings to potential targets, urging them to be aware of and prepared for potential attacks.[7]

33. Lurie Children's data security obligations were particularly important given the substantial increase in cyber and ransomware attacks and data breaches in the healthcare industry preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII/PHI retained in its servers. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000

[7] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974.

patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Lurie Children's knew or should have known that its electronic records would be targeted by cybercriminals.

34. Indeed, in 2022, Lurie Children's settled a case involving allegations that employees improperly accessed patient information between 2018 and 2019.[8] The settlement in that case required Lurie Children's to implement more robust security measures, but apparently, whatever measures Lurie Children's may have taken in response to that incident were inadequate.

35. Lurie Children's also derives substantial economic benefit from collecting Plaintiffs' and the Class Members' PII/PHI. Without the required submission of PII/PHI, Lurie Children's could not deliver its advertised services or obtain compensation from Plaintiffs and the Class Members as well as other payers. Lurie Children's knowingly accepted these benefits in exchange for the receipt of Plaintiffs' and the Class Members' PII/PHI.

D. Lurie Children's hackers to access its systems and seize PII/PHI.

36. Plaintiffs and the Class Members provided their PII/PHI to Lurie Children's with the reasonable expectation and mutual understanding that Lurie Children's would adhere to its promises to keep such information confidential and secure from unauthorized access. Plaintiffs and the Class Members relied on Lurie Children's to keep their PII/PHI confidential and securely maintained, to use their information for authorized business and healthcare purposes only, and to make only authorized disclosures of the information.

[8] Jill McKeon, *Lurie Children's Hospital Resolves Healthcare Data Breach Lawsuit*, Health IT Security (Nov. 9, 2022), https://healthitsecurity.com/news/lurie-childrens-hospital-resolves-healthcare-data-breach-lawsuit.

37. Plaintiffs and the Class Members took reasonable steps to maintain the confidentiality of their PII/PHI, but they relied on Lurie Children's sophistication and control over its own networks to keep their PII/PHI securely and confidentially maintained.

38. But despite its express promises to Plaintiffs and the Class Members, and its inherent duty to keep their PII/PHI safe, Lurie Children's allowed hackers to breach its systems, access Plaintiffs' and the Class Members' PII/PHI, and steal that data for their own, likely nefarious, purposes. The January 2024 attack reportedly took down Lurie Children's email, phones, and electronic health record systems, as well as its patient portal.

39. Subsequently, the Rhysida ransomware group listed Lurie Children's on its darknet extortion site, offering to sell data for 60 bitcoins (worth approximately $3.4 million).[9] Shortly thereafter, the site was updated to claim that "All data was sold."

40. Rhysida is a ransomware group that encrypts data on victims' computer systems and threatens to make it publicly available unless a ransom is paid.[10] In November 2023, the U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Multi-State Information Sharing and Analysis Center published an alert about Rhysida, warning that "threat actors leveraging Rhysida ransomware are known to impact 'targets of opportunity,' including victims in the education, healthcare, manufacturing, information technology, and government sectors."[11]

---

[9] Alexander Martin, *Ransomware gang claims to have made $3.4 million after attacking children's hospital*, The Record (Mar. 7, 2024), https://therecord.media/ransomware-gang-claims-payment-luries.

[10] Dan Milmo, *Rhysida, the new ransomware gang behind the British Library cyber-attack*, The Guardian (Nov. 24, 2023), https://www.theguardian.com/technology/2023/nov/24/rhysida-the-new-ransomware-gang-behind-british-library-cyber-attack.

[11] Cybersecurity & Infrastructure Security Agency, *CISA, FBI and MS-ISAC Release Advisory on Rhysida Ransomware* (Nov. 15, 2023), https://www.cisa.gov/news-events/alerts/2023/11/15/cisa-fbi-and-ms-isac-release-advisory-rhysida-ransomware.

E. Lurie Children's unreasonably waited months to alert victims of the Data Breach, and its notice was inadequate.

41. Although Lurie Children's admitted that it took systems offline in late January 2024 because of the breach, Lurie Children's waited until long after that to begin alerting victims of the breach.

42. Time is crucial when highly sensitive PII/PHI is subjected to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII/PHI of Plaintiffs and the Class Members may now be available on the Dark Web, for sale to criminals. As a result, Plaintiffs and the Class Members are currently and continuously exposed to the risk of fraud, identity theft, and misuse stemming from the potential publication of their PII. Lurie Children's delay in notifying victims was unreasonable and exacerbated Plaintiffs' and the Class Members' injuries.

43. In late June or early July 2024, Lurie Children's began sending Plaintiffs and other victims of the Data Breach a letter informing them, in relevant part, that their confidential PII/PHI had been accessed[12]:

> Through Lurie Children's' ongoing investigation, we have determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024. On January 31, 2024, to protect our systems and our ability to continue operations, Lurie Children's took certain electronic systems offline, including our email, phones, and electronic health record system (Epic), and its patient portal (MyChart). Lurie Children's also activated our standard incident response procedures, including the Hospital Incident Command Structure (HICS). The Hospital implemented its downtime procedures, and we have remained open for patient care throughout the investigation. Additionally, we retained leading cybersecurity experts and legal counsel to work with our internal teams. We have worked closely with law enforcement as well.
>
> Due to the complexity of the attack as well as our infrastructure, it has taken time to understand what happened and to identify the scope of impact to our systems and data. As part of our ongoing investigation, we thoroughly and methodically reviewed and analyzed impacted data contained on those systems. Through our investigation, Lurie Children's has determined that information relating to certain individuals, such as name,

[12] Lurie Children's Notifies Individuals of Data Breach, https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/.

> address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, prescription information, Social Security number, and telephone number, was impacted. The information relating to a particular individual varies individual to individual. We have no indication that the cybercriminals accessed data stored in our electronic health record system (Epic), although certain information stored in other Lurie Children's systems was impacted.

44. The notice letter omits crucial information. It does not describe the cause of the Data Breach, the vulnerabilities exploited, or the remedial measures taken to ensure such a breach does not happen again. Lurie Children's has never shared these critical details with Plaintiffs or the Class Members.

45. Instead, Lurie Children's has only stated vaguely it takes privacy "very seriously":

> **What are you doing to address this?**
>
> We take the privacy of our patients' and patient-families' information very seriously. We are working closely with security experts to continue our ongoing efforts to further enhance the security of our systems.

46. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts about the cause of the Data Breach or any remedial measures. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

47. Lurie Children's has also done next to nothing to prevent or mitigate further injury to Plaintiffs and the Class Members. The notice states that Lurie Children's will offer 24 months of credit monitoring services.

48. Two years of creditor monitoring is woefully inadequate in light of the serious damage to Plaintiffs' and the Class Members' privacy, and the present, imminent, and significant

risk of identity theft they now face. That risk, which is directly traceable to Lurie Children's reckless and negligent acts and omissions, will persist well beyond Lurie Children's arbitrary twelve month cap and can last a lifetime. Yet Lurie Children's has offered no additional safeguards to shield Plaintiffs or the Class Members from the enduring threats now facing them.

49. Instead, Lurie Children's purports to put the burden of identity protection on Plaintiffs and the Class Members—even though the harm they have suffered is Lurie Children's fault, not theirs. Lurie Children's notice warns Plaintiffs and the Class Members that they should "remain vigilant," "review your online accounts, financial statements, and Explanations of Benefits from your health insurers for any unauthorized activity."

50. Lurie Children's nowhere offers to compensate Plaintiffs or the Class Members for time spent on such activities, or reimburse them for money spent on such measures, although Lurie Children's own acts and omissions led directly to the need for such precautions.

F. Lurie Children's broke its promises to Plaintiffs and the Class Members and breached its duties to them.

i. Cyberattacks are preventable, but Lurie Children's failed to take appropriate steps to prevent the Data Breach.

51. When Lurie Children's allowed the Data Breach to occur, Lurie Children's broke its promises to Plaintiffs and the Class Members and breached its duties to protect their PII/PHI and maintain it securely. Despite the prevalence of public announcements of data breach and data security compromises, Lurie Children's failed to take appropriate steps to protect the PII/PHI of Plaintiffs and Class Members from being compromised.

52. Lurie Children's is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices, as well as state and federal laws governing data security.

53. Lurie Children's could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners—as it promised Plaintiffs and the Class Members it would, and as it had a duty to do.

54. Lurie Children's negligence in safeguarding Plaintiffs' and Class Members' PII/PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

55. Despite the prevalence of public announcements of data breaches and data security compromises, Lurie Children's failed to take appropriate steps to protect Plaintiffs' and the Class Members' PII/PHI from being compromised.

56. Lurie Children's failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI of Plaintiffs and Class Members.

57. Lurie Children's knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII/PHI.

58. Lurie Children's failed to provide adequate supervision and oversight of the PII/PHI with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiffs' and the Class Members' PII/PHI, misuse the PII/PHI, and disclose it to others without consent.

59. Lurie Children's failed to ensure the proper encryption of Plaintiffs' and Class Members' PII/PHI and monitor user behavior and activity to identify possible threats.

60. Lurie Children's failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

ii. Lurie Children's failed to follow FTC guidelines.

61. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[13] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Lurie Children's, should employ to protect against the unlawful exfiltration of PII/PHI.

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[14] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

63. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

64. The FTC recommends that companies not maintain PII/PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

[13] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed April 25, 2024).
[14] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://bit.ly/3u9mzre (last accessed June 25, 2024).

measures.[15]

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Lurie Children's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

iii. Lurie Children's failed to follow industry standards.

67. Despite its alleged commitments to securing sensitive data, Lurie Children's does not follow industry standard practices in securing PII/PHI.

68. Several best practices have been identified that at a minimum should be implemented by providers like Lurie Children's, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

69. Best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and

[15] *See Start With Security, A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 25, 2024).

routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

70. To prevent and detect cyber-attacks and/or ransomware attacks Lurie Children's could and should have implemented the following measures, as recommended by the United States Government:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary

folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

71. To prevent and detect cyber-attacks or ransomware attacks Lurie Children's also could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions
- Ensure collaboration among operations, security, and IT admins to configure servers and other endpoints securely;

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege
- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

[16] Department of Justice, *How to Protect Your Networks from RANSOMWARE* at 3, https://www.justice.gov/criminal/criminal-ccips/file/872771/dl (last accessed June 25, 2024).

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection; and
- Enable cloud-delivered protection.[17]

72. The occurrence of the Data Breach indicates that Lurie Children's failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII/PHI of nearly 512,000 individuals.

73. Lurie Children's failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. Such frameworks are the existing and applicable industry standards. Lurie Children's failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

75. Given that Lurie Children's was storing the sensitive PII/PHI of its clients' current and former patients, Lurie Children's could and should have implemented all of the above measures to prevent and detect cyberattacks.

iv. Lurie Children's failed to comply with HIPAA.

76. Lurie Children's is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed June 25, 2024).

Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

77. Lurie Children's is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[18] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

78. HIPAA's Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of health information.

79. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

80. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

81. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

82. HIPAA's Security Rule requires Lurie Children's to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such

[18] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

information that are not permitted; and

d. Ensure compliance by its workforce.

83. HIPAA also requires Lurie Children's to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Lurie Children's is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

84. HIPAA and HITECH also obligated Lurie Children's to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

85. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Lurie Children's to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[19]

86. Given that Lurie Children's was storing the sensitive PII/PHI of its clients' current and former patients, Lurie Children's could and should have implemented all of the above measures to prevent and detect cyberattacks. Its failure to implement one or more of the above is directly traceable to the Data Breach.

[19] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

G. Plaintiffs and the Class Members were harmed, and their injuries are traceable to Lurie Children's acts and omissions.

87. Plaintiffs and the Class Members would not have provided their PII/PHI to Lurie Children's had they known Lurie Children's would not keep it protected and confidential. Now, Plaintiffs and the Class Members have suffered actual injuries and damages as a result of the Data Breach. Plaintiffs and Class Members suffered actual injury from having their PII/PHI compromised in the Data Breach including (a) damage to and diminution in the value of their PII/PHI—a form of property that Lurie Children's obtained from Plaintiffs—as well as the value of their bargain with Lurie Children's; (b) lost time and money protecting themselves; (c) violation of their privacy rights and emotional distress; and (d) present and continuing injury arising from the increased risk of additional identity theft and fraud.

88. **Damage to and diminution in value of PII/PHI and benefit of the bargain.** Plaintiffs and the Class Members have suffered actual injury in the form of damages and diminution in the value of their PII/PHI – a form of intangible property that they entrusted to Lurie Children's. Plaintiffs and the Class Members also suffered from diminution of the value of their bargain with Lurie Children's, which included Lurie Children's promises to protect patients' PII/PHI consistent with state and federal law and Lurie Children's own Privacy Practices and Website Policy.

89. PII can be sold at prices exceeding $1,000.[20] A stolen credit or debit card number can sell for $15 to $110 on the Dark Web.[21] Criminals can also purchase access to entire

[20] Ryan Smith, *Revealed – How much is Personal information worth on the dark web?*, Insurance News (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.
[21] Miklos Zoltan, *Dark Web Price Index 2023*, Privacy Affairs (April 23, 2023), https://www.privacyaffairs.com/dark-web-price-index-2023/.

company data breaches for an average cost of between $2,000 to $4,000.[22]

90. Law-abiding consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

91. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[24]

92. Accordingly, any company that conducts business with a consumer and subsequently compromises the privacy of their PII effectively deprives that consumer of the full monetary value of their transaction with the company.

93. When agreeing to obtain medical services from Lurie Children's under certain terms, Plaintiffs, the Class Members, and other reasonable patients understood and expected that Lurie Children's would properly safeguard and protect their PII/PHI, when in fact, Lurie Children's did not provide the expected data security. Accordingly, Plaintiffs and the Class Members received medical services of a lesser value than what they reasonably expected to

---

[22] Kaspersky, *Cybercriminals sell access to companies via the Dark Web from $2000* (June 15, 2022), https://www.kaspersky.com/about/press-releases/2022_cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000.

[23] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) Information Systems Research 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1.

[24] *Medical I.D.Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%%2020use%20your,credit%20report%20may%20be%20affected.

receive under the bargains they struck with Lurie Children's.

94. **Lost time and money spent on mitigation.** Plaintiffs and the Class Members suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. Time is a compensable and valuable resource in the United States.

95. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis.[25]

96. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[26] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[27] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

97. Because of the Data Breach, Plaintiffs and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

98. When Lurie Children's finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Lurie Children's

[25] *Characteristics of minimum wage workers, 2020*, U.S. Bureau of Labor Statistics (Feb. 2021), https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm.
[26] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).
[27] *Id.*

notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who perpetrated the Data Breach, and the extent to which certain data elements were compromised. Had Plaintiffs and the Class Members been notified of the Data Breach in a timely manner and with greater specificity, they could have better attempted to mitigate their injuries. But Lurie Children's deprived them of that opportunity.

99. **Loss of privacy and emotional distress.** Plaintiffs and Class Members also suffered emotional distress because of the release of their PII/PHI—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII/PHI for nefarious purposes like identity theft and fraud.

100. **Severe, imminent risk of identity theft.** Plaintiffs and the Class Members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from theft of their PII/PHI. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

101. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[28]

[28] Anne Saita, *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

102. Moreover, "medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," according to Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[29]

103. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[30] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[31]

104. It can take victims years to spot or identify PII/PHI theft, giving criminals plenty of time to milk that information for cash.

105. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.[32]

---

[29] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft.

[30] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar, 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[31] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One,* Experian (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[32] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes,

106. Cyber-criminals can cross-reference two sources of personal information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

107. The development of "Fullz" packages means that stolen PII/PHI from the Data Breach can easily be linked with other information such as phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information was not included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

108. Plaintiffs and the Class Members have a continuing interest in ensuring that their PII/PHI, which upon information and belief remains backed up and in Lurie Children's possession, is protected and safeguarded from future breaches. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII/PHI.

CLASS ACTION ALLEGATIONS

109. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs proposes the following Classes, subject to amendment as appropriate:

> **Class: All persons in the United States whose PII/PHI was compromised in the Data Breach.**

---

including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," Krebs on Security (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

Illinois Subclass: All persons in Illinois whose PII/PHI was compromised in the Data Breach.

110. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

111. Plaintiffs hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

112. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, according to the reports submitted to the Office of the Maine Attorney General, approximately 512,000 persons were impacted in the Data Breach.

113. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII/PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach

were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII/PHI;

f. Whether Defendant breached its duty to Class Members to safeguard their PII/PHI;

g. Whether computer hackers obtained Class Members' PII/PHI in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached express and/or implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief;

o. Whether Defendant violated the Illinois Personal Information Protection Act;

p. Whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act; and

q. Whether Defendant violated the Illinois Uniform Deceptive Trade Practices Act.

114. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

116. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' PII/PHI was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

117. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Lurie Children's. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

118. Lurie Children's has acted on grounds that apply generally to the Class as a

whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

119. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

120. Lurie Children's owed a duty of care to Plaintiffs and the Class Members to use reasonable means to secure and safeguard the entrusted PII/PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These common law duties existed because Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices in Lurie Children's affirmative development and maintenance of its data security systems and its hiring of third-party providers entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiffs' and the Class Members' PII/PHI. In fact, not only was it foreseeable that Plaintiffs and the Class Members would be harmed by the failure to protect their PII/PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, Lurie Children's also knew that it was more likely than not that Plaintiffs and other Class Members would be harmed by such exposure and theft of their PII/PHI.

121. Lurie Children's duties to use reasonable security measures also arose from a special relationship with Plaintiffs and the Class Members as a result of being entrusted with their PII/PHI, which provided an independent duty of care. Plaintiffs' and the Class Members' PII/PHI was entrusted to Lurie Children's based on the understanding that Lurie Children's would take adequate security precautions. Moreover, Lurie Children's was capable of

protecting its network and systems, and the PII/PHI it stored on them, from unauthorized access, but failed to do so.

122. Lurie Children's breached its duties when it failed to use security practices that would protect the PII/PHI provided to it by Plaintiffs and the Class Members, thus resulting in unauthorized exposure and access to their PII/PHI.

123. Lurie Children's further breached its duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs' and the Class Members' PII/PHI within its possession, custody, and control.

124. As a direct and proximate cause of Lurie Children's failure to use appropriate security practices and failure to select a third-party provider with adequate data security measures, Plaintiffs' and the Class Members' PII/PHI was exposed, disseminated, and made available to unauthorized third parties.

125. Lurie Children's admitted that Plaintiffs' and the Class Members' PII/PHI was wrongfully disclosed as a result of the Data Breach.

126. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Lurie Children's knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that PII/PHI, and the necessity for encrypting PII/PHI stored on its systems.

127. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII/PHI would result in one or more types of injuries to Class Members.

128. But for Lurie Children's wrongful and negligent breach of its duties owed to

Plaintiffs and the Class Members, their PII/PHI would not have been compromised.

129. Neither Plaintiffs nor Class members contributed to the Data Breach or subsequent misuse of their PII/PHI as described in this Complaint.

130. The Data Breach caused direct and substantial damages to Plaintiffs and the Class Members, as well as the likelihood of future and imminent harm through the dissemination of their PII/PHI and the greatly enhanced and imminent risk of identity theft.

131. As a direct and proximate result of Lurie Children's negligence, Plaintiffs and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Lurie Children's, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class)

132. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

133. Lurie Children's owed a duty of care to Plaintiffs and the Class Members to use reasonable means to secure and safeguard the entrusted PII/PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These duties arose under the FTC Act and HIPAA.

134. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Lurie Children's of failing to use reasonable measures to protect PII/PHI.

135. Lurie Children's violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII/PHI and not complying with industry standards. Lurie Children's conduct was particularly unreasonable given the nature and amount of PII/PHI obtained and stored and the foreseeable consequences of a data breach.

136. Plaintiffs and the Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

137. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which caused the same harm suffered by Plaintiffs and the Class Members.

138. Lurie Children's duty to use reasonable security measures under HIPAA required Lurie Children's to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

139. For instance, HIPAA required Lurie Children's to notify victims of the Breach within 60 days of the discovery of the Data Breach. Lurie Children's did not begin to notify Plaintiffs or Class Members of the Data Breach until more than 60 days after it discovered the Data Breach.

140. Lurie Children's violation of Section 5 of the FTC Act (and similar state statutes) and HIPAA constitutes negligence *per se*.

141. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Lurie Children's knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that PII/PHI, and the necessity for encrypting PII/PHI stored on its systems.

142. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII/PHI would result in one or more types of injuries to Class Members.

143. But for Lurie Children's wrongful and negligent breach of its duties owed to Plaintiffs and the Class Members, their PII/PHI would not have been compromised.

144. Neither Plaintiffs nor Class members contributed to the Data Breach or subsequent misuse of their PII/PHI as described in this Complaint.

145. The Data Breach caused direct and substantial damages to Plaintiffs and the Class Members, as well as the likelihood of future and imminent harm through the dissemination of their PII/PHI and the greatly enhanced and imminent risk of identity theft.

146. As a direct and proximate result of Lurie Children's negligence, Plaintiffs and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly

impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Lurie Children's, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Class)

147. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

148. Plaintiffs and the Class Members entered into contracts with Lurie Children's when they obtained services from Lurie Children's, or otherwise provided PII/PHI to Lurie Children's.

149. As part of these transactions, Lurie Children's agreed to safeguard and protect the PII/PHI of Plaintiffs and the Class Members.

150. Lurie Children's expressly promised to Plaintiffs and the Class Members that:

a. "We are required by law to . . . assure that patient information that identifies you is kept confidential in accordance with law."

b. "[W]e must obtain your written authorization to use or disclose your patient information" (other than for specific, enumerated uses).

c. "We are committed to protecting the privacy of children."

d. "Lurie Children's is committed to maintaining reasonable physical, technical, and administrative measures to protect your personal information."

e. "We will retain your personal data for as long as necessary to accomplish the purpose for which it was collected unless a longer period is required by law or needed to resolve a dispute or protect our legal rights."

151. Lurie Children's also promised that it will only share patients' PII/PHI in specific scenarios that are identified in the Privacy Practices and Website Policy.

152. These promises to Plaintiffs and the Class Members formed the basis of the bargain between Plaintiffs and the Class Members, on the one hand, and Lurie Children's, on the other.

153. Plaintiffs and the Class Members would not have provided their PII/PHI to Lurie Children's had they known that Lurie Children's would not safeguard their PII/PHI.

154. Plaintiffs and the Class Members fully performed their obligations under their contracts with Lurie Children's. But Lurie Children's breached its contracts with Plaintiffs and the Class Members by failing to safeguard Plaintiffs' and the Class Members' PII/PHI.

155. As a direct and proximate result of Lurie Children's breach of contract, Plaintiffs and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses

and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT IV
***IN THE ALTERNATIVE*—BREACH OF IMPLIED CONTRACT**
(On Behalf of Plaintiffs and the Class)

156. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

157. Plaintiffs allege Count IV in the alternative to Count III.

158. Plaintiffs and the Class Members entered into an implied contract with Lurie Children's when they obtained services from Lurie Children's, or otherwise provided PII/PHI to Lurie Children's.

159. As part of these transactions, Lurie Children's agreed to safeguard and protect the PII/PHI of Plaintiffs and the Class Members.

160. Plaintiffs and the Class Members entered into the implied contracts with the reasonable expectation that Lurie Children's data security practices and policies were reasonable and consistent with legal requirements and industry standards.

161. Plaintiffs and the Class Members would not have provided and entrusted their PII/PHI to Lurie Children's in the absence of the implied contract or implied terms between them and Lurie Children's. The safeguarding of the PII/PHI of Plaintiffs and the Class Members was part of the basis of the parties' bargain.

162. Plaintiffs and the Class Members fully performed their obligations under the

implied contracts with Lurie Children's.

163. Lurie Children's breached their implied contracts with Plaintiffs and the Class Members to protect their PII/PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) allowed the theft of that information by unauthorized third parties.

164. As a direct and proximate result of Lurie Children's breach of implied contract, Plaintiffs and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT V
***IN THE ALTERNATIVE*—UNJUST ENRICHMENT**
(On behalf of Plaintiffs and the Class)

165. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth

above and incorporate them at this point by reference as though set forth in full.

166. Plaintiffs allege Count V in the alternative to Count III above.

167. Plaintiffs and the Class Members have an interest, both equitable and legal, in the PII they provided Lurie Children's and that was ultimately stolen in the Data Breach.

168. Lurie Children's benefitted from receiving Plaintiffs' and the Class Members' PII/PHI, and by its ability to retain, use, sell, and profit from that information. Lurie Children's accepted and was aware of the benefits conferred upon it by Plaintiffs and the Class Members.

169. Lurie Children's also understood and appreciated that the PII/PHI pertaining to Plaintiffs and the Class Members was private and confidential and its value depended upon Lurie Children's maintaining the privacy and confidentiality of that PII/PHI except as expressly agreed.

170. But for Lurie Children's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and the Class Members would not have provided PII/PHI to Lurie Children's or would not have permitted Lurie Children's to gather additional PII/PHI.

171. Plaintiffs' and the Class Members' PII/PHI has an independent value to Lurie Children's. Lurie Children's was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create through the use of Plaintiffs' and the Class Members' PII/PHI.

172. Due to Lurie Children's's actions, Lurie Children's also unjustly obtained benefits equivalent to the disparity in value between the payments made for services with reasonable data privacy and security measures, and the services received, which lacked such measures.

173. Lurie Children's also unjustly obtained benefits equal to the value of Plaintiffs'

and the Class Members' PII/PHI.

174. It is inequitable, unfair, and unjust for Lurie Children's to retain these wrongfully obtained benefits. Lurie Children's's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

175. The benefit conferred upon, received, and enjoyed by Lurie Children's was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Lurie Children's to retain the benefit.

176. Lurie Children's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and the Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII/PHI and has caused the Plaintiffs and the Class Members other damages as described herein.

177. Plaintiffs and the Class Members have no adequate remedy at law.

178. Lurie Children's is therefore liable to Plaintiffs and the Class Members for restitution or disgorgement in the amount of the benefit conferred on Lurie Children's as a result of its wrongful conduct, including specifically: the value to Lurie Children's of the PII that was stolen in the Data Breach; the profits Lurie Children's received and is receiving from the use of that information; and the amounts that Lurie Children's overcharged Plaintiffs and the Class Members for use of Lurie Children's products and services.

COUNT VI
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

179. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

180. Lurie Children's invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII/PHI and by negligently

maintaining the confidentiality of Plaintiffs' and Class Members' PII/PHI, as set forth above. Lurie Children's further invaded Plaintiffs' and Class Member's privacy by allowing third parties to give publicity to Plaintiffs' and Class Members sensitive and confidential PII/PHI by among other things posting it online.

181. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' PII/PHI was disclosed without prior written authorization of Plaintiffs and the Class.

182. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class Members provided and disclosed their PII/PHI to Lurie Children's privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

183. As a direct and proximate result of Lurie Children's above acts, Plaintiffs' and the Class Members' PII/PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages as described herein.

184. Lurie Children's has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII/PHI with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

185. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Lurie Children's may freely treat Plaintiffs' and Class Members' PII/PHI with sub-standard and insufficient protections.

186. Unless and until enjoined, and restrained by order of this Court, Lurie Children's wrongful conduct will continue to cause Plaintiffs and the Class Members great and irreparable injury in that the PII/PHI maintained by Lurie Children's can be viewed, printed, distributed, and used by unauthorized persons.

COUNT VII
VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT
815 Ill. Comp. Stat. §§ 530/10(a) *et seq.*
(On Behalf of Plaintiffs and the Illinois Subclass)

187. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

188. Plaintiffs bring this claim on behalf of themselves and the Illinois Subclass.

189. Lurie Children's is a Data Collector as defined in the Illinois Personal Information Protection Act ("ILPIPA"), 815 Ill. Comp. Stat. § 530/5.

190. Lurie Children's is a Data Collector that owns or licenses computerized data that includes "health insurance information," "medical information," and "personal information," as defined in ILPIPA, 815 Ill. Comp. Stat. § 530/5. Lurie Children's also maintains computerized data that includes "health insurance information," "medical information," and "personal information," as defined in ILPIPA, that Lurie Children's does not own.

191. Plaintiffs' and the Illinois Subclass Members' PII/PHI includes "Personal Information," "Health Insurance Information," and "Medical Information," as defined by 815 Ill. Comp. Stat. § 530/5.

192. The ILPIPA requires Lurie Children's to give immediate notice of breach of a security system to owners of Personal Information that Lurie Children's does not own or license, including Plaintiffs and the Illinois Subclass Members.

193. Lurie Children's failed to give immediate notice of the Data Breach to Plaintiffs and the Illinois Subclass Members. That failure violated 815 Ill. Comp. Stat. § 530/10(b).

194. The ILPIPA also requires Lurie Children's to notify Plaintiffs and the Illinois Subclass Members of a breach of its data security system that may have compromised Personal

Information which Lurie Children's owns or licenses in the most expedient time possible and without unreasonable delay.

195. Lurie Children's failed to provide notice of the Data Breach to Plaintiffs and the Illinois Subclass Members expediently and without unreasonable delay. That failure violated 815 Ill. Comp. Stat. § 530/10(a).

196. Violating ILPIPA is an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

197. As a direct and proximate result of Lurie Children's violations of ILPIPA, Plaintiffs and the Illinois Subclass Members have suffered, and will continue to suffer, damages and other actual and ascertainable losses of money or property, and monetary and non-monetary damages and harm, including but not limited to: (i) a substantially increased risk of identity theft, necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money spent mitigating and remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

198. Plaintiffs and the Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered due to Lurie Children's violations of ILPIPA, including equitable relief, costs, and attorneys' fees.

COUNT VIII
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 Ill. Comp. Stat. §§ 505 *et seq.*
(On Behalf of Plaintiffs and the Illinois Subclass)

199. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

200. Plaintiffs bring this claim on behalf of themselves and the Illinois Subclass.

201. Lurie Children's is a "person" as defined by the Illinois Consumer Fraud and

Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. § 505/1(c).

202. Plaintiffs and the Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. § 505/1(e).

203. Lurie Children's conduct as described in this Complaint was in the conduct of "trade" or "commerce" as defined in 815 Ill. Comp. Stat. § 505/1(f).

204. Lurie Children's engaged in deceptive acts or practices in the conduct of its trade or commerce in violation of the ICFA, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Illinois Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including the duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect Plaintiffs' and the Illinois Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including duties imposed by HIPAA, the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not

properly secure Plaintiffs' and the Illinois Subclass Members' PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*

205. Lurie Children's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Lurie Children's data security and its ability to protect Plaintiffs' and the Illinois Subclass Members' PII/PHI.

206. The above unfair and deceptive practices and acts by Lurie Children's were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Illinois Subclass that they could not reasonably avoid; and the substantial injury outweighed any benefits to consumers or to competition.

207. As a direct and proximate result of Lurie Children's unlawful and deceptive acts and practices, Plaintiffs and the Illinois Subclass Members have suffered, and will continue to suffer, damages and other actual and ascertainable losses of money or property, and monetary and non-monetary damages and harm, including but not limited to: (i) a substantially increased risk of identity theft, necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money spent mitigating and remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

208. Plaintiffs and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT IX
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §§ 510 *et seq.*
(On Behalf of Plaintiffs and the Illinois Subclass)

209. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

210. Plaintiffs bring this claim on behalf of themselves and the Illinois Subclass.

211. Lurie Children's is a "person" as defined by the Illinois Uniform Deceptive Trade Practices Act ("IUDTPA"), 815 Ill. Comp. Stat. § 510/1(5).

212. Lurie Children's engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. § 510/2(a), including:

a. Representing that goods or services have characteristics they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

213. Lurie Children's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Illinois Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including the duties imposed by HIPAA, the FTC Act, 15 U.S.C. § 45, the IUDTPA, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*, which was a

direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect Plaintiffs' and the Illinois Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the IUDTPA, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and the Illinois Subclass Members' PII/PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PII/PHI, including duties imposed by HIPAA, the FTC Act, 15 U.S.C. § 45, the IUDTPA, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*

214. Lurie Children's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Lurie Children's data security and its ability to protect Plaintiffs' and the Illinois Subclass Members' PII/PHI.

215. The above unfair and deceptive practices and acts by Lurie Children's were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Illinois Subclass that they could not reasonably avoid; and the substantial injury outweighed any benefits to consumers or to competition.

216. As a direct and proximate result of Lurie Children's unlawful and deceptive acts and practices, Plaintiffs and the Illinois Subclass Members have suffered, and will continue to suffer, damages and other actual and ascertainable losses of money or property, and monetary and non-monetary damages and harm, including but not limited to: (i) a substantially increased risk of identity theft, necessitating expenditures for protective and remedial services for which they are

entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI for which there is a well-established national and international market; (v) lost time and money spent mitigating and remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

217. Plaintiffs and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Lurie Children's as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and Illinois Subclass as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the proposed Class;

B. For injunctive and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

D. For an award of restitution or disgorgement, in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury on all triable issues.

///

DATED: July 3, 2024

Respectfully submitted,

/s/ Hassan A. Zavareei
Hassan A. Zavareei (Bar No. 456161)
Katherine M. Aizpuru (*pro hac vice forthcoming*)
David W. Lawler (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
hzavareei@tzlegal.com
kaizpuru@tzlegal.com
dlawler@tzlegal.com

Counsel for Plaintiffs and the Proposed Class